(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 March 2001 (01.03.2001)

PCT

(10) International Publication Number
WO 01/15440 A1

(51) International Patent Classification⁷: H04N 5/76

(21) International Application Number: PCT/US00/22353

(22) International Filing Date: 15 August 2000 (15.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/149,999 20 August 1999 (20.08.1999) US

(71) Applicant *(for all designated States except US)*: **DIGITAL NOW, INC.** [US/US]; Suite 140, 8401 Old Courthouse Road, Vienna, VA 22182 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **REED, William, G.** [US/US]; 9804 62nd Avenue South, Seattle, WA 98118 (US).

(74) Agent: **REISTER, Andrea, G.**; Covington & Burling, 1201 Pennsylvania Avenue, N.W., Washington, DC 20004-2401 (US).

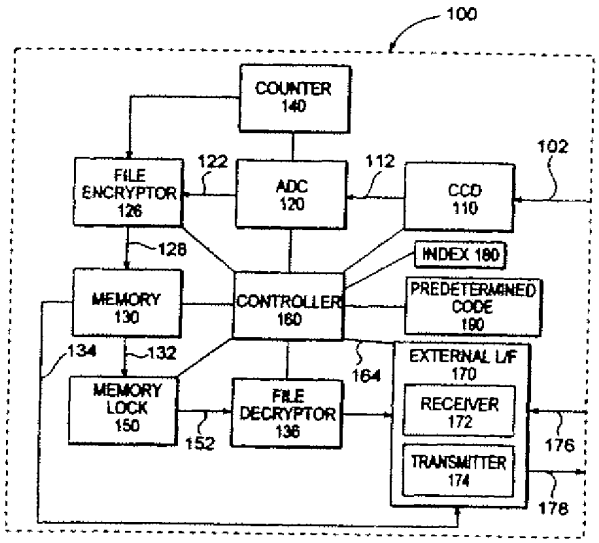
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ONE TIME USE DIGITAL CAMERA



(57) Abstract: Apparatus and method for preventing unauthorized access or erasure of digital image files stored in the memory (130) of a digital camera (100) used for taking motion still photographs, motion pictures, etc., while permitting an authorized person to access, erase and/or reset the camera (100) for further use. Access and erasure of the digital files is enabled only when a predetermined authorization signal (126), code or decryption key (136) is received via an external interface (170).

WO 01/15440 A1

ONE TIME USE DIGITAL CAMERA

FIELD OF THE INVENTION

The present invention relates generally to the field of photography, and more particularly to digital photography. Still more particularly, the present invention relates to "authorized-access only" digital cameras, which contain security devices that prevent the digital images stored in their memories from being accessed, printed, downloaded, erased, etc. without authorization.

RELATED ART

Driven by rapid advances in image quality and the steadily falling prices of cameras, computers and color printers, digital photography is becoming more and more popular as a means of capturing, sharing and displaying images, such as still photographs, motion picture videos, etc. Digital photography differs from conventional photography in that visual images are captured and stored electronically rather than on traditional film. For example, a digital camera can use a charge-coupled device (CCD) element to capture an image through the lens when the operator presses a button. The circuitry within the camera then stores the image captured by the CCD in a storage medium such as solid-state "flash memory" cards and "sticks," or removable hard drives, DVD, CDROM and floppy diskettes. After the image has been captured, it is typically "downloaded" to a computer by cable (or by wireless transmission) or, in the case of DVDs, CDROMs, floppy diskettes, flash cards or memory sticks, "uploaded" to a computer, printer or other device. Once stored on a computer, the image can be manipulated, processed and printed much like the image from a scanner or related input device.

One of the strong appeals of digital photography is the control consumers have over the digitized images. Consumers can instantly print photos or watch videos, or share them with friends, family members, customers and colleagues by sending the images via electronic mail ("email") or by posting them on the Internet. For a small investment in software, consumers can edit, resize, duplicate and repair images, apply special effects, change and improve colors, classify and organize images into electronic scrapbooks and even create slide shows. Tools within these software programs also make

it easy to prepare images for use in do-it-yourself presentations, newsletters, business plans, greeting cards, calendars and invitations.

People want pictures, not cameras. Thus, disposable and recyclable film cameras, which do not offer all the advantages of digital photography described above, are well known in the photography business. A disposable film camera is designed to be used by a single consumer for exposing a single roll of film. The camera is typically thrown away or destroyed after the roll of film has been removed for processing. A recyclable camera is not discarded after the film is removed. Instead, the camera is rebuilt or re-conditioned—usually by the manufacturer—so that it can make additional images, and then put back on the market for re-sale to a different consumer. Recyclable cameras are often called disposable, "single-use" or "one-time use" cameras, even though they are designed to be recycled and "re-used," albeit by a different consumer.

When the maximum number of exposures available on the filmstrip inside a disposable or recyclable camera is reached, the camera is given to a photofinisher for processing. Processing the exposed roll of film requires breaking open the body of the camera to remove the film cartridge, thereby rendering certain parts of the camera useless. So the photofinisher either discards the camera or forwards it to a third party for recycling, refurbishing, remanufacturing, etc.

Disposable and recyclable film cameras are less expensive than regular film cameras. As such, they are an attractive option for consumers who want to have pictures, but do not want to purchase or own, or simply cannot afford, a more expensive camera. Disposable and recyclable cameras are also a good, low-cost solution for consumers who, for example, forget to take their regular cameras with them while they are traveling, or simply want to avoid the hassle and inconvenience of packing and carrying expensive camera equipment around while on the road. With a disposable or recyclable camera, the consumer can economically and conveniently purchase, use and dispose of the camera while at the travel destination.

Recyclable film cameras are commercially viable for manufacturers because the cameras can be re-sold multiple times before they are eventually discarded, thereby allowing the manufacturer to recoup the manufacturing and marketing costs and make a profit. In addition, because they are typically designed so that only authorized photofinishers can remove and process the film, recyclable camera manufacturers count

on making money through the film processing fees. But there are some significant problems associated with conventional recyclable cameras.

Several problems arise when recyclable film cameras are recycled by unauthorized persons. Cameras recycled by an unauthorized person may be of lesser quality than cameras recycled by an authorized person. Moreover, when a camera is recycled by an unauthorized person, the camera manufacturer cannot derive additional revenue through multiple sales of that camera or through film processing fees. Attempts to address these problems, at least insofar as conventional recyclable film cameras are concerned, are discussed in U.S. Pat. No. 4,890,130, issued Dec. 26, 1989, U.S. Pat. No. 5,418,585, issued May 23, 1995, U.S. Pat. No. 5,517,265, issued May 14, 1996, and U.S. Pat. No. 5,708,855, issued Jan. 13, 1998, which are incorporated herein by reference.

Each of these patents offers solutions for preventing unauthorized recycling of conventional film cameras—usually by destroying some part of the camera when the filmstrip is advanced to the next frame for the next exposure or when the cartridge is removed from the camera for processing. But none of the foregoing patents provides a solution for preventing unauthorized recycling of digital cameras, or unauthorized processing of digital image files captured using digital cameras.

Although some of the less sophisticated, lower resolution digital camera models are now priced to compete with some of the high-end film cameras, the potential for unauthorized image processing and unauthorized recycling of digital cameras has made it commercially impractical to manufacture and sell digital cameras that are recyclable.

Accordingly, there is a need recognized by inventors in the industry for preventing unauthorized access to digital images stored in a digital camera in order to make in-expensive recyclable digital cameras commercially viable.

SUMMARY OF THE INVENTION

The present invention is directed to an apparatus and method for preventing unauthorized access or erasure of digital files stored in the memory of a digital camera, while permitting an authorized person to access, erase and/or reset the camera for further use. In one aspect of the present invention, a camera is provided that comprises a memory, means for recording an image, means for converting the image into a digital

file, means for storing the digital file in the memory, means for detecting a predetermined authorization signal, and means for preventing access to the digital file when the predetermined authorization signal is not detected. In the preferred embodiments, the mode of operation according to the present invention is to prevent access when the predetermined signal is not detected. A person of ordinary skill in the art would recognize that the same result could be achieved by alternate means, such as allowing access only when a predetermined authorization signal is detected. Such alternate means are considered within the scope of the present invention.

The camera according to the present invention can also comprise an external interface for receiving authorization signals, and a controller, coupled to the external interface, for monitoring incoming authorization signals and identifying the predetermined authorization signal.

In a further aspect of the present invention, the camera also includes a counter for tracking a number of images recorded, means for inhibiting certain functions of the camera (such as the image-capture, analog-to-digital conversion or file storage functions) when the counter reaches a predetermined value, and means for preventing the counter from being reset while the predetermined authorization signal is not detected. In yet a further aspect of the present invention, the camera comprises a memory, means for recording an image, means for converting the image into a digital file, means for storing the digital file in the memory, means, responsive only to the detection of a predetermined authorization signal, for transmitting the digital file out of the memory to an external device.

In still a further aspect of the present invention, a method or process for unloading files contained in a camera is provided. The method comprises the steps of: providing a predetermined authorization signal to the camera via an external interface; enabling access to a memory in the camera containing the files upon receipt of the predetermined authorization signal; and transmitting the files from the memory to an external device. The method can also comprise resetting an image counter and/or removing the predetermined authorization signal from the external interface. In a further aspect of the present invention, a method of controlling access to files contained in a camera is provided. This method comprises the steps of: monitoring an external interface for the presence of a predetermined authorization signal, and upon

receipt of the predetermined authorization signal, enabling access to a memory in the camera containing the files. This method may also include the step of transmitting the digital files to an external device.

Features and Advantages of the Present Invention

It is a feature of the present invention that it monitors an external interface for authorization signals and detects a predetermined authorization signal.

It is another feature of the present invention that it prevents access to stored digital files unless a predetermined authorization signal is detected.

It is a further feature of the present invention that the contents of the camera memory cannot be accessed, transmitted to an external device or erased unless a predetermined authorization signal is detected.

It is yet a further feature of the present invention that it accommodates the use of an encrypted predetermined authorization signal.

It is a further feature of the present invention that it accommodates the use of any one of a variety of mechanical, electronic, optical and wireless interfaces for producing a predetermined authorization signal.

It is a further feature of the present invention that it displays an error message when an authorization signal other than the predetermined authorization signal is detected.

It is still a further feature of the present invention that certain functions are disabled when a counter reaches a predetermined value, and the counter cannot be reset unless a predetermined authorization signal is detected.

An advantage of the present invention is that only an authorized person can access, transmit, print or erase digital files stored in memory. In addition, only such an authorized person can restore the camera to the fully operational mode after the image counter has reached a predetermined value.

A further advantage of the present invention is that no parts of the device need to be disassembled, discarded, replaced or repaired in order to remove and process the digital files contained in its memory or to restore the camera to its fully-operational mode after processing the digital images.

Another advantage of the present invention is that it makes low-cost disposable digital cameras a commercially viable marketing concept based on the fact that the

manufacturers, or their designated authorized agents, are the only entities capable of processing the digital files and recycling the cameras for further use. Thus, the manufacturing and distribution costs of such cameras are recovered at least in part by a guaranteed stream of income generated from multiple photo-finishing service fees.

Still a further advantage of the present invention is that it can easily be adapted to allow users to take and print only a prepaid number of pictures.

Additional features and advantages of the invention are set forth in part in the description that follows, and in part are apparent from the description, or may be learned by practice of the invention. The features and advantages of the invention may also be realized and attained by means of the instrumentalities and combinations particularly set out in the appended claims.

BRIEF DESCRIPTION OF THE FIGURES

The accompanying drawings, which are incorporated in and constitute part of the specification, illustrate preferred embodiments of the invention, and, together with the description, serve to explain the principles of the present invention. In the drawings, like reference numbers indicate identical or functionally similar elements. Additionally, the left-most digit(s) of a reference number identifies the drawing in which the reference number first appears.

FIG. 1 shows a block diagram of one embodiment of a camera according to the present invention.

FIG. 2 depicts a block diagram of another preferred embodiment of the present invention wherein the predetermined authorization signal is received from a secure server over an interconnected computer network connection.

FIGs. 3A and 3B show a flow diagram for unloading files from a camera and resetting camera parameters in accordance with the present invention.

FIG. 4 depicts an exemplary computer system, suitable for use with the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Reference will now be made in detail to the preferred embodiments of the invention, examples of which are illustrated in the accompanying drawings. Notably, the present invention may be implemented using software, hardware or any combination thereof, as would be apparent to those of ordinary skill in the art, and the figures and examples below are not meant to limit the scope of the present invention or its embodiments or equivalents.

Overview of the Present Invention

The present invention makes disposable, recyclable and single-use digital cameras commercially viable for camera manufacturers, which in turn allows consumers to have pictures, video, etc. without having to own the camera used to make them. The present invention also makes it possible for a consumer to have digital features and technology without giving up the advantages of using a "disposable" camera. The present invention will also help make a number of new consumer services possible. With the present invention, for example, a consumer who has captured images using a recyclable digital camera can have their images uploaded, processed, printed, mailed and/or e-mailed to their home or to distant relatives simply by connecting the camera containing the images to a special kiosk owned or authorized by the camera manufacturer. As another example, amusement park operator could provide an embodiment of a camera according to the present invention, to arriving patrons to be used by the patrons only while visiting the park. Such temporary amusement park cameras could be further configured to transmit images over a wireless network connection to printers placed at or near the amusement park's exit gates so that the images can be retrieved by the patrons upon exit. As another example, a real estate broker could use the present invention to take still pictures or video of a piece of property and have those images transmitted to the broker's office or directly to potential buyers.

The present invention is directed to an apparatus and method for preventing unauthorized access or erasure of digital files stored in the memory of a digital camera, but permitting an authorized person to access, print or transmit the digital files out of the memory and optionally reset an image counter on the camera for further use. In a typical system according to the present invention, a charge-coupled device (CCD) containing light-sensitive photoelectric diodes is used to receive and capture light

reflected from visual images outside the system. In an alternative embodiment, a CMOS (Complimentary Metal-Oxide Semiconductor) image sensor array, preferably with on-board controllers, could be used to receive and capture the visual images. An analog-to-digital converter (ADC) converts the analog signals to digital signals that are stored in a memory.

In a preferred embodiment, the digital file is encrypted before storing the file in memory using encryption methods known in the art, such as the "public key" encryption method. A decryption processor is also provided, which will decrypt the digital file only upon receipt of a predetermined decryption key. The decryption processor may reside inside the camera, or it may be located in a separate personal computer "(PC") or other device where the encrypted digital files have been transferred or stored via an external interface on the camera or via a removable memory device, such as a flash memory card, memory stick, removable hard drive, DVD, CDROM or floppy diskette. The PC may be the user's own home personal computer, or it may be built into a publicly available kiosk provided for these purposes. In a preferred embodiment, the user may connect either the camera or the removable storage device to the home or kiosk PC.

If the encrypted digital files reside on a removable storage device, or inside a home or kiosk PC, they cannot be accessed, viewed, printed or decrypted until the decryption processor receives a predetermined decryption key. If the encrypted digital files still reside on the camera, they cannot be printed, decrypted or erased from memory, but they can be viewed on the built-in preview screen of the camera, if so equipped. In order to receive the predetermined decryption key, a connection between the home or kiosk PC and a secure server is established via the Internet or some other computer network. Once the connection is established, an index is sent to the secure server. The secure server contains a list of randomly generated encryption/decryption keys, which are accessed according to the indexes embedded in the cameras. When a home or kiosk PC sends an index to the secure server, the secure server uses the index to fetch the predetermined decryption key for that particular camera from the list of decryption keys. The decryption key is then sent back to the home or kiosk PC, where the decryption processor uses it to decrypt the images for viewing, printing, editing, etc.

By having a large number of indexes and keys that are randomly assigned to the cameras as they are manufactured, a high level of security is achieved. If the index number or decryption key for one camera falls into the hands of an unauthorized person, other cameras that require different indexes and decryption keys are not compromised. It should be recognized by those of skill in the art that the predetermined decryption key may also be used by the camera to signify authorized access status, which not only allows decryption, but also allows the camera to be reset (i.e., recycled) for further use.

Alternatively, rather than or in addition to containing a list of predetermined decryption keys, the secure server may contain a list of access codes, which are also ordered by index. In such an embodiment, the secure server is configured to use the index to fetch a predetermined access code and the camera is configured to prevent decryption of image files and/or recycling of the camera unless and until the predetermined access code is received.

It should also be recognized that an even higher level of security could be achieved by configuring the camera to use a different randomly generated index every time it is recycled or every time the stored images are removed. In this way, only a limited number of images from the camera will be accessible to an unauthorized person who somehow gains access to a camera's index or decryption key.

In yet another preferred embodiment, the memory is equipped with a memory lock, which prevents the digital files from being transmitted from the camera absent detection of a predetermined authorization signal. An external interface is provided for receiving authorization signals from an external source. When the authorization signals are received by the external interface, they are passed to a controller, coupled to the external interface, which processes the signals and detects when the predetermined authorization signal is present. When the presence of the predetermined authorization signal is detected, the controller generates a signal that disengages the memory lock, thereby allowing the digital files stored in the memory to be accessed, transmitted and/or erased.

The apparatus may also include an image counter, which is incremented (or decremented, as the case may be) each time an image is captured, converted or stored in memory. The controller monitors the value of the counter. When the counter reaches a certain predetermined value—such as "20," for example, in the case of an incrementing

counter, or "0" in the case of a decrementing counter—the controller can be configured to disable one or more essential functions of the camera, such as the image capture, conversion or memory store. The controller may also be configured to allow the counter to be re-initialized when the predetermined authorization signal is detected.

The present invention is also directed to a method or process for unloading files contained in a digital camera. The first step is to provide a predetermined authorization signal to the camera via an external interface, thereby enabling access and/or erasure of the digital files contained in the camera's memory. In a preferred embodiment, this step may be preceded by transmission of an index to the external device seeking access so the external device can use the index to fetch a predetermined access code from a list of randomly generated access codes. When the predetermined access code is received, the digital files are transmitted, using one of a variety of transmission means, from the memory to the external device. The process may also optionally include the steps of resetting the image counter on the camera and/or removing the predetermined authorization signal from the external interface.

The present invention is still further directed to a process for controlling access to files contained in a camera. This process includes the step of monitoring the external interface for the presence of a predetermined authorization signal. Upon receipt of the predetermined authorization signal, memory access is enabled so that the digital files can be read, transmitted or erased. This process may also optionally include the step of transmitting the digital files to an external device.

Detailed Operation of the Present Invention

With reference now to FIG. 1, a block diagram of one embodiment of a camera 100 in accordance with the present invention is shown. A charge-coupled device (CCD) 110 or a CMOS image sensor array (not shown) is used to capture a visual image entering CCD 110 at aperture 102 according to methods generally well known in the art. In a preferred embodiment, CCD 110 is comprised of a matrix array of photo sensitive sites and transfer shift registers to transfer the captured photo current to a digitization system. A particularly preferred CCD for use with the present invention is a Panasonic MN39571PT 2.3 mega-pixel image sensor. It is understood that the present invention is

not limited to use with such a CCD, and can be used with other CCDs or other facilities that capture visual images.

Analog signals from CCD 110 are passed via link 112 to an analog-to-digital converter (ADC) 120, where they are "digitized," i.e., converted to binary or digital signals, for use by a computer or electronic processor. In one embodiment, ADC 120 is implemented using the CS7620 Digital Camera Front End Chip available from Cirrus Logic.

In a preferred embodiment, the digital output from ADC 120 is coupled to file encryptor 126 via a link 122, so that the digital signals, which now represent the captured image, are encrypted before being stored in memory 130. Algorithms suitable for encrypting digital image files are well known in the industry. For example, the "public key" system of encryption would provide a reasonably strong level of protection against unauthorized access.

In a preferred embodiment, each camera is randomly assigned an encryption "key" when it was manufactured. The camera will use that randomly assigned encryption key for every digital image file it encrypts. To gain access to the encrypted digital image files, the same key that was used for encryption—or a key that "corresponds" to the encryption key—must be used in the decryption algorithm. Encryption and decryption keys, however, are neither shipped with camera 100, nor disclosed to the public. Instead, the camera manufacturer and/or its authorized agents keep secret the list of decryption keys corresponding to the cameras.

After the digital image files are encrypted, they are sent to the camera's memory 130 via link 128. Memory 130 could be implemented in a variety of ways, including the use of standard semiconductor memory, magnetic disks or magnetic tape. Memory 130 may also be implemented with removable storage devices, such as flash memory cards, memory sticks, removable hard disk drives, DVDs, CDROMs, floppy diskettes, or a combination of all or any of these devices.

External interface 170 is coupled via links 176 and 178 to an external device (not depicted in FIG. 1) configured to transmit authorization signals to camera 100 and receive the digital files when they are transmitted out of the camera 100. In a most preferred embodiment of the present invention, external interface 170 comprises a wireless communications interface having: (a) a wireless receiver 172, for receiving

authorization signals and commands from the external device; and (b) a wireless transmitter 174, for transmitting digital files and status and error messages, if necessary, to the external device.

External interface 170 may be implemented with infrared signals, in which case receiver 172 is an infrared receiver and transmitter 174 is an infrared transmitter, or it could be implemented with radio frequency signals, in which case receiver 172 is a radio receiver and transmitter 174 is a radio transmitter. Another option is to implement external interface 170 with optical signals, in which case receiver 172 is photoelectric diode and transmitter 174 is a light-emitting diode (LED). Finally, external interface 170 could be implemented using electric or electronic signals (not pictured in FIG. 1), in which case an electric or electronic connector suitable for receiving one end of an electronic cord replaces receiver 172 and transmitter 174 in external interface 170. As can be seen in FIG. 1, external interface 170 is coupled to a controller 160 via link 164. In the preferred embodiment, controller 160 causes a machine-readable index 180 to be transmitted to the external device via external interface 170. The external device then uses the index to look up and retrieve the correct decryption key from a list of keys, which may reside on or be accessible to the external device. When controller 160 has received the correct decryption key, the encrypted digital image files are transmitted from memory 130 to file decryptor 136, where they are decrypted and then transmitted out of the camera 100 through the external interface 170 to the external device.

In another embodiment of the present invention, controller 160 performs the encryption and decryption functions. In still another embodiment, the present invention is configured to operate without encryption and decryption. For example, in one embodiment, controller 160 monitors signals from external interface 170 via link 164 and detects when the signal matches a predetermined code 190 stored in camera 100 by the manufacturer. The external device may send the predetermined code upon establishing a connection channel with camera 100. Alternatively, the external device can be configured to send the predetermined code 190 in response to receiving an index from the camera 100.

If the predetermined code is detected, the digital image files are transmitted out of memory 130 to external interface 170 via link 134, and then out of camera 100 to the external device via link 178. If the authorization signals received

through the external interface 170 do not match predetermined code 190, controller 160 will not allow the digital files stored in memory 130 to be transmitted out of camera 100. In a preferred embodiment, CCD 110, ADC 120 and memory 130 are coupled to a counter 140, which keeps track of the number of images captured by CCD 110, the number of images converted by ADC 120, the number digital files stored in memory 130, the number of digital files capable of being stored in the as yet unused portion of memory 130, or all or any combination of the above. As CCD 110 and ADC 120 capture images, controller 160 monitors the values of the counter 140. When the number of images captured equals a predetermined maximum image count, or when memory 130 reaches its full capacity, controller 160 prevents further operation of the image capture and digital file storage functions. Thus, the camera 100 will stop functioning until the counter 140, if present, is reset, or until some or all of the digital files have been removed from memory 130. In a preferred embodiment, controller 160 will also prevent counter 140 from being changed or reset unless a decryption key or predetermined code 190 is detected on the external interface 170 or the correct decryption key is received.

In another embodiment of the present invention, controller 160 performs the forgoing the image-counting functions. In still another embodiment, the present invention is configured without a counter 140 or other device that performs image-counting functions. One of ordinary skill in the art would recognize that counter 140 may be incremented toward a maximum value or, alternatively, decremented toward a minimum value (usually "0"), without departing from the scope of the present invention.

In an alternative embodiment of the present invention, restricted access to the digital image files may be implemented by means of a memory lock 150, which is coupled to memory 130 via link 132 and file decryptor 136 via link 152. When camera 100 is not being used to capture images, controller 160 "locks" memory 130 using memory lock 150. Memory lock 150 functions by preventing the digital files stored in memory 130 from being transmitted out of camera 100. In a preferred embodiment, memory lock 150 does not, however, prevent display of the digital files on a built-in preview screen of camera 100, if so equipped.

Memory lock 150 may be implemented in software, hardware or a combination of both. If memory lock 150 is implemented in software, then the portion of the software code used to read, change, erase or transmit digital files out of camera 100

will not execute. If memory lock 150 is implemented in hardware, then an electronic signal is sent to a non-volatile gating circuit, where it is converted to voltage output, which is then used to shut off the semiconductor or magnetic memory in memory 130, or prevent memory 130 from starting up in the first place.

In another embodiment of the present invention, controller 160 performs the memory locking functions. In still another embodiment, the present invention is configured without a memory lock 150 or other device that performs memory-locking functions. If camera 100 is only equipped with removable memory, for example, then implementing the memory lock function would not be the best solution for securing the digital files because the digital files may have already been removed from the camera. In these cases, encrypting the digital files before storing them in memory 130, as discussed above, is a better solution for preventing unauthorized access to those files.

With reference now to FIG. 2, a more complete description of the preferred embodiment of the present invention is provided. Camera 100 is used to capture, digitize, encrypt and store one or more images. The encrypted digital files are stored on memory 130, which may be fixed within camera 100 or comprised of some form of removable memory, such as a flash memory card, a memory stick, a removable hard disk drive, DVD, CD or a floppy diskette. When the user is ready to unload the digital images from camera 100, in order to print or email them to relatives, for example, the user connects camera 100 to a personal computer (PC) 202 configured to receive commands and digital images from camera 100 via external interface 170 and links 176 and 178. In the preferred embodiment, external interface 170 is an infrared communications port, or some other wireless communication device, comprising a transmitter and a receiver, as depicted in FIG. 1.

Alternatively, if memory 130 is removable, then the user simply takes the memory 130 out of camera 100 and inserts it directly into PC 202 via input/output port 206. In either case, the encrypted digital files may, but not necessarily, be transferred from the removable memory 130 to storage medium 210 residing on PC 202 via link 208. However, the digital images contained in the digital files cannot be accessed, viewed or printed because they are still encrypted. In the preferred embodiment, PC 202 may be the user's home personal computer or a publicly available kiosk containing a personal computer. If PC 202 is a public kiosk, it is even more desirable to have a wireless

communication channel, depicted as links 176 and 178 in FIGs. 1 and 2, between camera 100 (external interface 170) and PC 202. A wireless communication channel would minimize the extreme wear and tear that would occur on the connectors if camera 100 had to be connected to the kiosk by an electronic interface cord.

PC 202 is comprised of an input/output port 206, a storage medium 210, a processor 214 and an interface to a computer network, depicted in FIG. 2 as network interface 220. As stated above, input/output port 206, in the preferred embodiment, comprises a wireless communication device, such as an infrared transmitter and receiver. However, input/output port 206 may also be configured to couple to camera 100 via an electronic connection, such as a Universal Serial Bus ("USB") cable, or to accept a removable memory device from camera 100, such as a flash memory card. PC 202 may also be attached via link 222 to a printer 228 capable of printing digital files after they have been decrypted.

Input/output 206 is coupled via link 208 to storage medium 210, which will usually, but not necessarily, be comprised of a very large capacity memory device, such as a hard disk, CD-ROM or DVD-ROM. A network interface 220, such as a modem, local area network interface card and/or a T1 wide area interface, is also provided, so that PC 202 can communicate with remote computers coupled to an interconnected computer network, such as the Internet.

Finally, PC 202 incorporates a processor 214, which is coupled to input/output port 206, storage medium 210, network interface 220 and printer 228. In a preferred embodiment of the present invention, processor 214 is comprised of a software program and graphical user interface that automates and simplifies the process of uploading, decrypting, viewing, classifying, emailing, printing and storing visual images captured with camera 100. For these purposes, a decryption processor will likely but not necessarily be incorporated processor 214. A decryption processor may not be necessary, for example, if camera 100 has its own decryptor (depicted in FIG. 1 as file decryptor 136), the digital files are still residing in memory 130 of camera 100, and camera 100 is still in communication with PC 202 via external interface 170. On the other hand, a decryption processor running on PC 202 would be required if camera 100 was no longer in communication with PC 202. Processor 214 could also be comprised of a standard

Internet browsing program, or a browser plug-in, configured to operate for the purposes described herein.

In a preferred embodiment, PC 202 is configured to establish a connection over an interconnected computer network 207 to a secure server 204 operated by camera 100's manufacturer, or an authorized agent of the manufacturer, via communication links 232 and 234. The secure server 204 is comprised of a control logic 250 and a look-up table 260. Control logic 250 is configured to operate in cooperation with commands and data provided by processor 214 via communication links 232 and 234. Control logic 250 is coupled via link 252 to look-up table 260. Look-up table 260 preferably contains a list of decryption keys ordered and accessed by the same indexes that are embedded in the cameras. In an alternative embodiment, look-up table 260 contains a list of predetermined codes, which may also be ordered and accessed by the same indexes. Once camera 100 is connected to PC 202 and a connection is established between PC 202 and secure server 204 via links 232 and 234, processor 214 sends an index to control logic 250. Control logic 250 uses the index to retrieve the key corresponding to camera 100 from look-up table 260. Control logic 250 sends the key back to processor 214, where a decryption processor incorporated into processor 214 retrieves the encrypted digital files from storage medium 210 and uses the key to decrypt the digital files. The unencrypted digital files are then stored on storage medium 210 for subsequent viewing, printing, editing, etc. If the encrypted digital files are not yet located in storage medium 210, processor 214 causes the encrypted digital files to be transmitted from memory 130 of camera 100 after receiving the decryption key but before the decryption process is initiated.

In another embodiment of the present invention, camera 100 is not equipped with a removable memory function and the digital image files, which may not be encrypted, cannot be transmitted from camera 100 to PC 202 unless and until camera 100 receives a predetermined code via external interface 170. In this case, rather than sending a key to processor 214 in response to the transmittal of the index, control logic 250 sends a predetermined code. The processor 214 passes the predetermined code, which may be comprised of numbers, letters, other characters, or some combination of letters, numbers or other characters, to camera 100 via input/output port 206 and external interface 170. When camera 100 detects the presence of the predetermined code, the

unencrypted digital files are then transmitted out of memory 130 and into storage medium 210 for subsequent viewing, printing, emailing, editing, etc.

In yet another embodiment of the present invention, camera 100 itself has a network interface, preferably wireless, which allows camera 100 to communicate directly with an interconnected computer network, like the Internet, instead of a PC. In this embodiment, upon receipt of the predetermined code, controller 160 (depicted in FIG. 1) causes the digital files to be transmitted out of memory 130 to a remote computer via a wireless communication channel coupled to the network interface. In this embodiment, no PC or kiosk is required for removing the digital files from camera 100.

In a preferred embodiment, the receipt of the predetermined code initiates an authorized access mode in camera 100 wherein certain operational parameters, such as the authorization code, the image counter, the maximum number of images and maximum resolution, can be changed or reset as appropriate. Authorized access mode would also allow erasure of the digital files from memory 130 after copies of the files have been transmitted to an external device.

With reference now to FIGs. 3A and 3B, a more complete description of a method for unloading files contained in a camera in accordance with the present invention is provided. The first step, depicted as STEP 302 in flowchart 300 in FIG. 3A, is to provide a predetermined authorization signal to the camera via an external interface. The predetermined authorization signal may be generated by supplying a numeric or alphanumeric code, or an electrical, optical, magnetic, radio or infrared signal to the external interface. The signal may be detected by means of a receiver.

Upon receipt of the predetermined authorization signal, the next step, STEP 304, is to enable access to a memory in the camera containing the files. Removing or disengaging facilities that prevent access to the memory, such as encryption or a memory lock, accomplishes this step. The final step, STEP 306, is to transmit the files from the memory to an external device.

In a preferred embodiment, the method of unloading files includes initiation of an authorized access mode, where the operator has an opportunity to reset or modify certain operational parameters of the camera, as depicted in the flow diagram contained in FIG. 3B. The first step, STEP 308, is to determine whether to enter the authorized access mode. If the answer is no, the image counter is reset and authorized

access mode is terminated in a STEP 318. However, if the answer is yes, the operator then has an opportunity to change the authorization signal, STEP 310, the maximum image count, STEP 312, the maximum memory capacity, STEP 314, and the image resolution, STEP 316. Processing then proceeds to STEP 318 to reset the image counter.

With reference now to FIG. 4, a more complete description of a computer system suitable for use with the preferred embodiment of the present invention is provided. The computer system 402 includes one or more processors, such as a processor 404. The processor 404 is connected to a communication bus 406. Various software embodiments are described in terms of this exemplary computer system. After reading this description, it will become apparent to a person skilled in the relevant art how to implement the invention using other computer systems and/or computer architectures.

The computer system 402 also includes a main memory 408, preferably random access memory (RAM), and can also include a secondary memory 410. The secondary memory 410 can include, for example, a hard disk drive 412 and/or a removable storage drive 414, a DVD drive, a CDROM drive, a floppy disk drive, a magnetic tape drive, an optical disk drive, etc. The removable storage drive 414 reads from and/or writes to a removable storage unit 418 in a well-known manner. The removable storage unit 418, represents a floppy disk, DVD, CDROM, magnetic tape, optical disk, etc. which is read by and written to by the removable storage drive 414. As will be appreciated, the removable storage unit 418 includes a computer usable storage medium having stored therein computer software and/or data.

In alternative embodiments, the secondary memory 410 may include other similar means for allowing computer programs or other instructions to be loaded into the computer system 802. Such means can include, for example, a removable storage unit 422 and an interface 420. Examples of such can include a program cartridge and cartridge interface (such as that found in video game devices), a removable memory chip (such as an EPROM, or PROM) and associated socket, and other removable storage units 422 and interfaces 420 which allow software and data to be transferred from the removable storage unit 422 to the computer system 402.

The computer system 402 can also include a communications interface 424. The communications interface 424 allows software and data to be transferred between the computer system 402 and external devices. Examples of the

communications interface 424 can include a modem, a network interface (such as an Ethernet card), a communications port, a PCMCIA slot and card, etc. Software and data transferred via the communications interface 424 are in the form of signals 426 that can be electronic, electromagnetic, optical or other signals capable of being received by the communications interface 424. Signals 426 are provided to communications interface via a channel 428. A channel 428 carries signals 426 and can be implemented using wire or cable, fiber optics, a phone line, a cellular phone link, an RF link and other communications channels.

In this document, the terms "computer program medium" and "computer usable medium" are used to generally refer to media such as the removable storage device 418, a hard disk installed in hard disk drive 412, and signals 426. These computer program products are means for providing software to the computer system 402. Computer programs (also called computer control logic) are stored in the main memory 408 and/or the secondary memory 410. Computer programs can also be received via the communications interface 424. Such computer programs, when executed, enable the computer system 402 to perform the features of the present invention as discussed herein. In particular, the computer programs, when executed, enable the processor 404 to perform the features of the present invention. Accordingly, such computer programs represent controllers of the computer system 402.

In an embodiment where the invention is implemented using software, the software may be stored in a computer program product and loaded into the computer system 402 using the removable storage drive 414, the hard drive 412 or the communications interface 424. The control logic (software), when executed by the processor 404, causes the processor 404 to perform the functions of the invention as described herein.

In another embodiment, the invention is implemented primarily in hardware using, for example, hardware components such as application specific integrated circuits (ASICs). Implementation of such a hardware state machine so as to perform the functions described herein will be apparent to persons skilled in the relevant art(s).

In yet another embodiment, the invention is implemented using a combination of both hardware and software.

The present invention has been disclosed and described herein in what is considered to be its most preferred embodiments. It should be noted that variations and equivalents may occur to those skilled in the art upon reading the present disclosure and that such variations and equivalents are intended to come within the scope of the invention and the appended claims.

CLAIMS

I claim:

1. A camera, comprising:

a memory;

means for recording an image;

means for converting said image into a digital file;

means for storing said digital file in said memory;

means for detecting a predetermined authorization signal; and

means for preventing access to said digital file when said predetermined authorization signal is not detected.

2. The camera of claim 1, wherein said memory comprises a memory stick.

3. The camera of claim 1, wherein said memory comprises a flash memory card.

4. The camera of claim 1, wherein said memory comprises a hard drive.

5. The camera of claim 1, wherein said memory comprises a floppy diskette.

6. The camera of claim 1, wherein said means for recording an image comprises:

a lightproof enclosure having an aperture;

an array, disposed within said lightproof enclosure, comprising a plurality of light-sensitive photo-electric cells; and

a lens, positioned over said aperture, through which light is focused on said array and recorded by said photo-electric cells.

7. The camera of claim 1, wherein:

said digital file is encrypted; and

said means for allowing access to said digital file comprises means for decrypting said digital file, and a decryption key.

8. The camera of claim 1, wherein said means for detecting said predetermined authorization signal comprises:

an external interface for receiving authorization signals; and

a controller, coupled to said external interface, wherein said controller monitors said authorization signals and identifies said predetermined authorization signal.

9. The camera of claim 1, wherein said means for detecting said predetermined authorization signal comprises an authorization code processor.

10. The camera of claim 1, wherein said means for detecting said predetermined authorization signal comprises an optical, infrared or radio frequency interface.

11. The camera of claims 9 or 10, wherein said means for detecting said predetermined authorization signal further comprises:
a decryption processor; and
a decryption key.

12. The camera of claim 1, wherein said means for preventing access to said digital file comprises:

a memory lock, coupled to said memory, said memory lock configured to prohibit reading said digital file.

13. The camera of claim 1, further comprising:

a counter for tracking a number of images recorded;

means for inhibiting said means for recording an image when said counter reaches a predetermined value; and

means for preventing said counter from being reset when said predetermined authorization signal is not detected.

14. The camera of claim 1, further comprising:

a counter for tracking a number of images recorded;

means for inhibiting said means for converting said image into said digital file when said counter reaches a predetermined value; and

means for preventing said counter from being reset when said predetermined authorization signal is not detected.

15. The camera of claim 1, further comprising:

a counter for tracking a number of images recorded;

means for inhibiting said means for storing a digital file when said counter reaches a predetermined value; and

means for preventing said counter from being reset when said predetermined authorization signal is not detected.

16. A camera, comprising:

a memory;

means for recording an image;

means for converting said image into a digital file;

means for storing said digital file in said memory;

means for detecting a predetermined authorization signal; and

means for preventing transmission of said digital file out of said camera when said predetermined authorization signal is not detected.

17. The camera of claim 16, wherein said means for recording an image comprises:

a lightproof enclosure having an aperture;

an array, disposed within said lightproof enclosure, comprising a plurality of light-sensitive photo-electric cells; and

a lens, positioned over said aperture, through which light is focused on said array and recorded by said photo-electric cells.

18. A camera, comprising:

a memory;

means for recording an image;

means for converting said image into a digital file;

means for storing said digital file in said memory;

means, responsive only to the detection of a predetermined authorization signal, for transmitting said digital file out of said camera to an external device.

19. The camera of claim 18, wherein said means for recording an image comprises:

a lightproof enclosure having an aperture;

an array, disposed within said lightproof enclosure, comprising a plurality of light-sensitive photo-electric cells; and

a lens, positioned over said aperture, through which light is focused on said array and recorded by said photo-electric cells.

20. The camera of claim 18, wherein said means for transmitting comprises a transmitter configured for communication via a link to a computer network.

21. The camera of claim 18, wherein said means for transmitting comprises a transmitter configured for communication via a radio signal.

22. The camera of claim 18, wherein said means for transmitting comprises a transmitter configured for communication via an infrared radiation signal.

23. The camera of claim 18, wherein said means for transmitting comprises a transmitter configured for communication via an optical signal.

24. The camera of claim 18, further comprising a connector for direct connection with said external device.

25. The camera of claim 18, wherein said means for recording an image comprises:

a lightproof enclosure having an aperture;

an array, disposed within said lightproof enclosure, comprising a plurality of light-sensitive photo-electric cells; and

a lens, positioned over said aperture, through which light is focused on said array and recorded by said photo-electric cells.

26. A camera, comprising:

a memory;

means for recording a image;

means for converting said image into a digital file;

means for storing said digital file in said memory;

means for detecting a predetermined authorization signal; and

means for allowing access to said digital file only when said predetermined authorization signal is detected.

27. The camera of claim 26, wherein said means for recording an image comprises:

a lightproof enclosure having an aperture;

an array, disposed within said lightproof enclosure, comprising a plurality of light-sensitive photo-electric cells; and

a lens, positioned over said aperture, through which light is focused on said array and recorded by said photo-electric cells.

28. The camera of claim 26, wherein:

said digital file is encrypted; and

said means for allowing access to said digital file comprises means for decrypting said digital file, and a decryption key.

29. The camera of claim 26, wherein said means for detecting said predetermined authorization signal comprises:

an external interface for receiving authorization signals; and

a controller, coupled to said external interface, wherein said controller monitors said authorization signals and identifies said predetermined authorization signal.

30. The camera of claim 29, wherein said predetermined authorization signal further comprises a predetermined code.

31. The camera of claim 30, wherein said means for detecting said predetermined authorization signal further comprises:

an index; and

means for transmitting said index to an external device via said external interface.

32. The camera of claim 26, wherein said means for detecting said predetermined authorization signal comprises a code processor.

33. The camera of claim 26, wherein said means for detecting said predetermined authorization signal comprises an optical, infrared or radio frequency interface.

34. The camera of claims 32 or 33, wherein said means for detecting said predetermined authorization signal further comprises:

a decryption processor; and

a decryption key.

35. The camera of claim 26, further comprising

a counter for tracking a number of images recorded;

means for inhibiting said means for recording an image when said counter reaches a predetermined value; and

means for allowing said counter to be reset only when said predetermined authorization signal is detected.

36. The camera of claim 26, further comprising

a counter for tracking a number of images recorded;

means for inhibiting said means for converting said image into said digital file when said counter reaches a predetermined value; and

means for allowing said counter to be reset only when said predetermined authorization signal is detected.

37. The camera of claim 26, further comprising

a counter for tracking a number of images recorded;

means for inhibiting said means for storing a digital file when said counter reaches a predetermined value; and

means for allowing said counter to be reset only when said predetermined authorization signal is detected.

38. A camera, comprising:

a memory;

means for recording a image;

means for converting said image into an encrypted digital file;

means for storing said encrypted digital file in said memory;

means for detecting authorized access to said digital file comprising a predetermined code, an external interface configured for receiving codes, and a controller, coupled to said external interface, wherein said controller monitors said codes and determines when one of said codes matches said predetermined code; and

means, responsive to said controller, for decrypting said encrypted digital file.

39. The camera of claim 38, wherein said means for detecting authorized access further comprises:

an index; and

means for transmitting said index to an external device via said external interface.

40. The camera of claim 38, further comprising means for transmitting said digital file out of said camera to an external device.

41. The camera of claim 38, 39 or 40, further comprising:

an image counter; and

means for re-initializing said image counter.

42. A method of unloading files contained in a camera, comprising the steps of:

providing a predetermined authorization signal to said camera via an external interface;

upon receipt of said predetermined authorization signal, enabling access to a memory in the camera containing said files; and

transmitting said files from said memory to an external device.

43. The method recited in claim 42, further comprising transmitting an index to said external device prior to said providing step.

44. The method recited in claim 42, further comprising the step of resetting an image counter.

45. The method recited in claim 42, further comprising the step of removing said predetermined authorization signal from said external interface.

46. The method recited in claim 42, wherein said predetermined authorization signal is generated by entering a predetermined number into said camera.

47. The method recited in claim 42, wherein said predetermined authorization signal is generated by entering a predetermined string of characters into said camera.

48. The method recited in claim 42, wherein said predetermined authorization signal is provided to said camera via an electrical, optical, infrared or radio frequency interface.

49. The methods of claims 46, 47 or 48, further comprising the step of decrypting an authorization signal.

50. The method recited in claim 42, further comprising the step of erasing said memory.

51. The method recited in claim 42, further comprising the step of changing said predetermined authorization signal.

52. The method recited in claim 42, further comprising the step of changing a maximum value of said image counter.

53. The method recited in claim 42, further comprising the step of changing a maximum capacity of said memory.

54. The method recited in claim 42, further comprising the step of changing a maximum resolution of said digital camera.

55. The method recited in claim 42, further comprising the step of displaying a message upon receiving an authorization signal other than said predetermined authorization signal.

56. A method of unloading files contained in a camera, comprising the steps of:

providing a predetermined authorization signal to said camera via an external interface;

upon receipt of said predetermined authorization signal, enabling access to a memory in the camera containing said files;

transmitting said files from said memory to an external device;

resetting an image counter; and

removing said predetermined authorization signal from said external interface.

57. The method recited in claim 56, further comprising transmitting an index to said external device prior to said providing step.

58. A method of controlling access to files contained in a camera, comprising the steps of:

monitoring an external interface for the presence of a predetermined authorization signal; and

upon receipt of said predetermined authorization signal, enabling access to a memory in the camera containing said files.

59. The method recited in claim 58, further comprising transmitting an index to said external device prior to said providing step.

60. The method recited in claim 58, further comprising the step of disabling access to said memory containing said files upon removal of said predetermined authorization signal from said external device.

61. The method recited in claim 58, further comprising the step of transmitting said files from said memory to an external device.

62. The method recited in claim 58, further comprising the step of resetting an image counter.

63. The method recited in claim 58, wherein said predetermined authorization signal is generated by entering a predetermined number into said camera.

64. The method recited in claim 58, wherein said predetermined authorization signal is generated by entering a predetermined string of characters into said camera.

65. The method recited in claim 58, wherein said predetermined authorization signal is provided to said camera via an electrical, magnetic, optical, infrared or radio frequency interface.

66. The methods of claims 63, 64 or 65, further comprising the step of decrypting an authorization signal.

67. The method recited in claim 58, further comprising the step of erasing a memory.

68. The method recited in claim 58, further comprising the step of changing said predetermined authorization signal.

69. The method recited in claim 58, further comprising the step of changing a maximum allowable value of said image counter.

70. The method recited in claim 58, further comprising the step of changing a maximum capacity of said memory.

71. The method recited in claim 58, further comprising the step of changing a maximum resolution of said digital camera.

72. The method recited in claim 58, further comprising the step of displaying a message upon receiving an authorization signal other than said predetermined authorization signal.

73. A method of unloading files contained in a camera, comprising the steps of:

providing a predetermined code to said camera via an external interface;

upon receipt of said predetermined code, enabling access to a memory in the camera containing said files;

transmitting said files from said memory to an external device; and

resetting an image counter.

74. The method recited in claim 73, further comprising transmitting an index to said external device prior to said providing step.

75. A method of unloading encrypted files contained in a camera, comprising the steps of:

providing a predetermined code to said camera via an external interface;

upon receipt of said predetermined code, decrypting said encrypted files;

transmitting said decrypted files from said memory to an external device; and

resetting an image counter.

76. The method recited in claim 75, further comprising transmitting an index to said external device prior to said providing step.

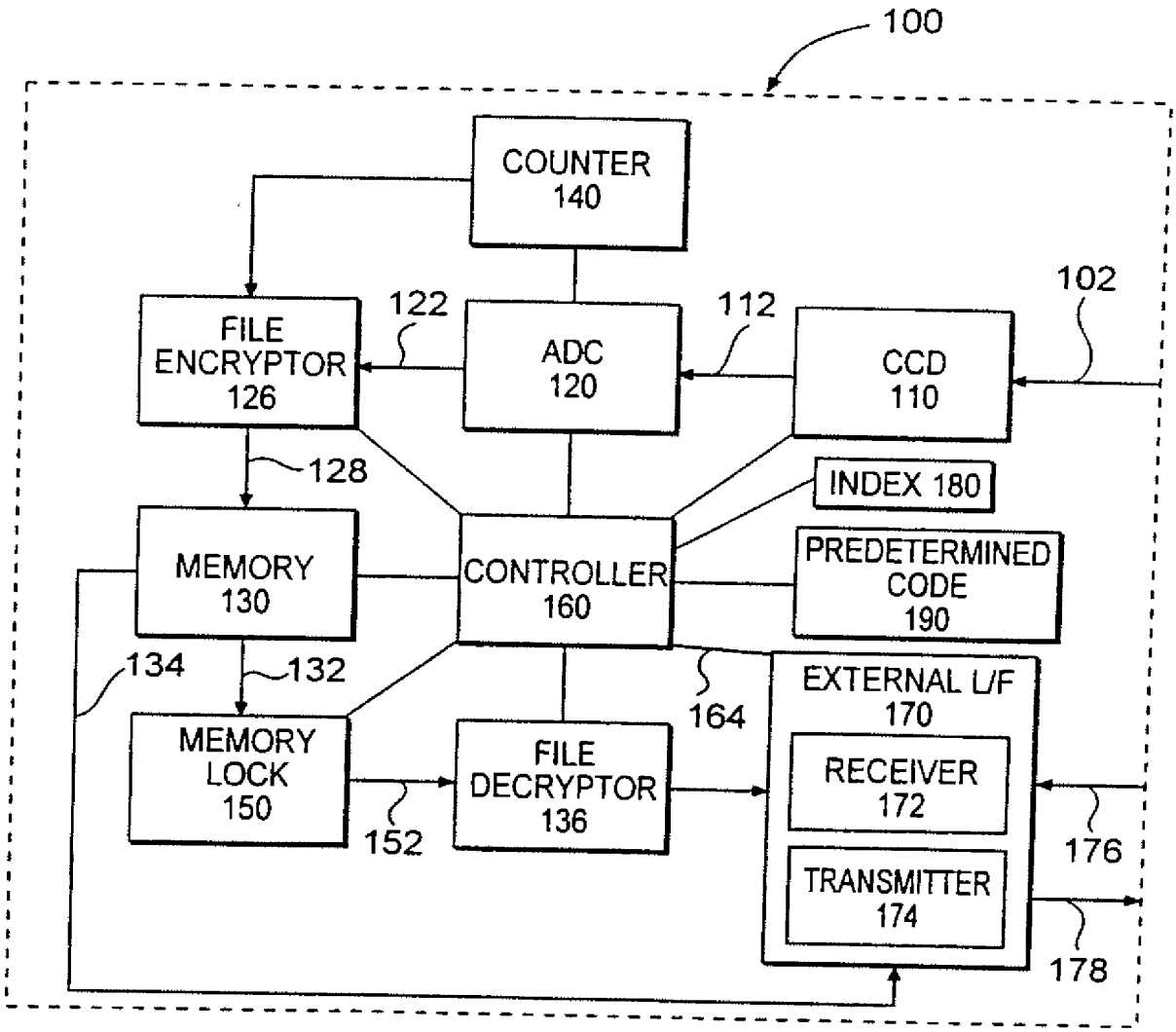

100
COUNTER
140
FILE
ENCRYPTOR
126
122
ADC
120
112
CCD
110
102
128
INDEX 180
MEMORY
130
CONTROLLER
160
PREDETERMINED
CODE
190
134
132
164
EXTERNAL I/F
170
MEMORY
LOCK
150
152
FILE
DECRYPTOR
136
RECEIVER
172
176
TRANSMITTER
174
178

FIG. 1

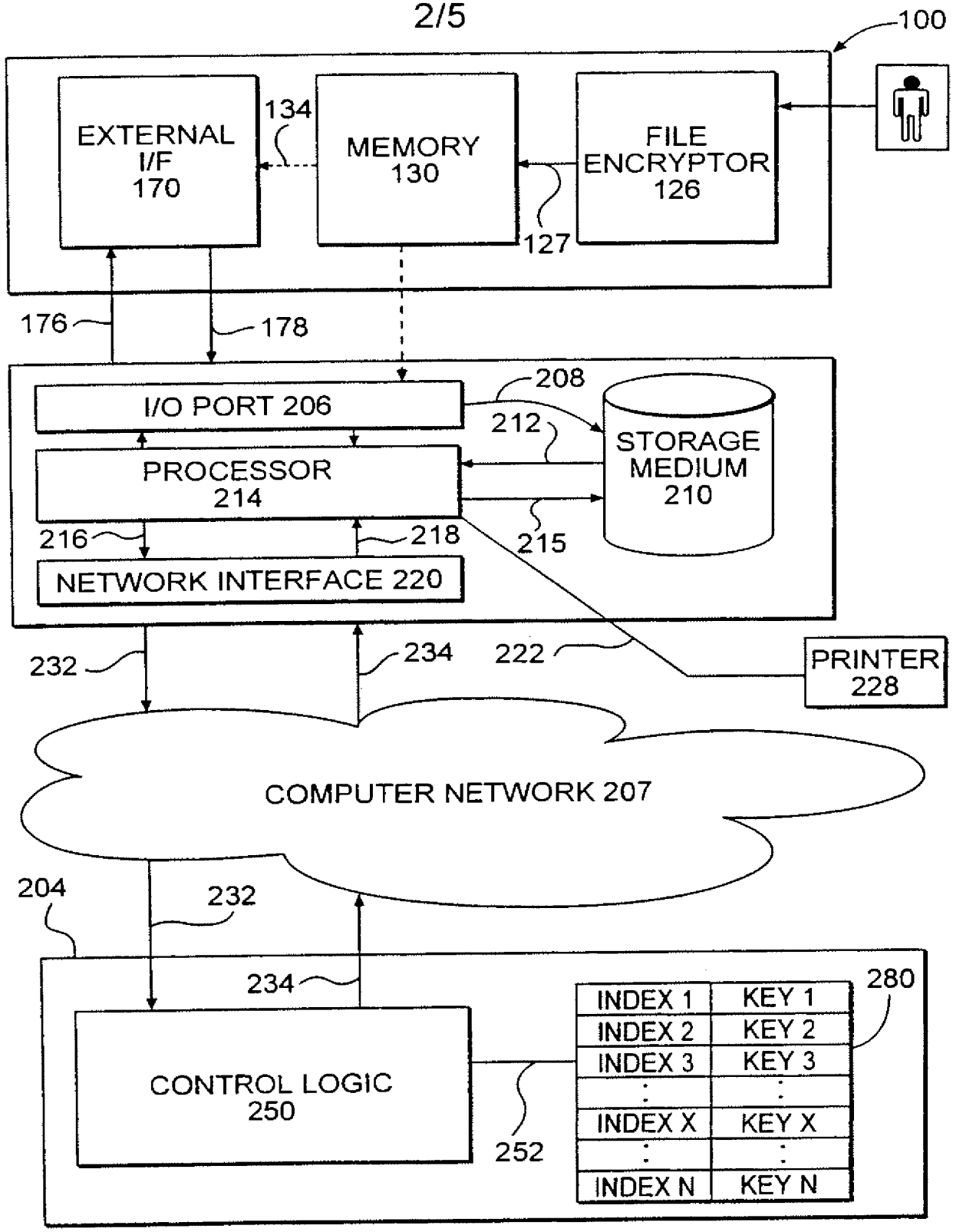

100
EXTERNAL I/F 170
134
MEMORY 130
FILE ENCRYPTOR 126
127
176
178
I/O PORT 206
208
212
STORAGE MEDIUM 210
PROCESSOR 214
216
218
215
NETWORK INTERFACE 220
232
234
222
PRINTER 228
COMPUTER NETWORK 207
204
232
234
280
CONTROL LOGIC 250
252
INDEX 1
KEY 1
INDEX 2
KEY 2
INDEX 3
KEY 3
INDEX X
KEY X
INDEX N
KEY N

FIG. 2

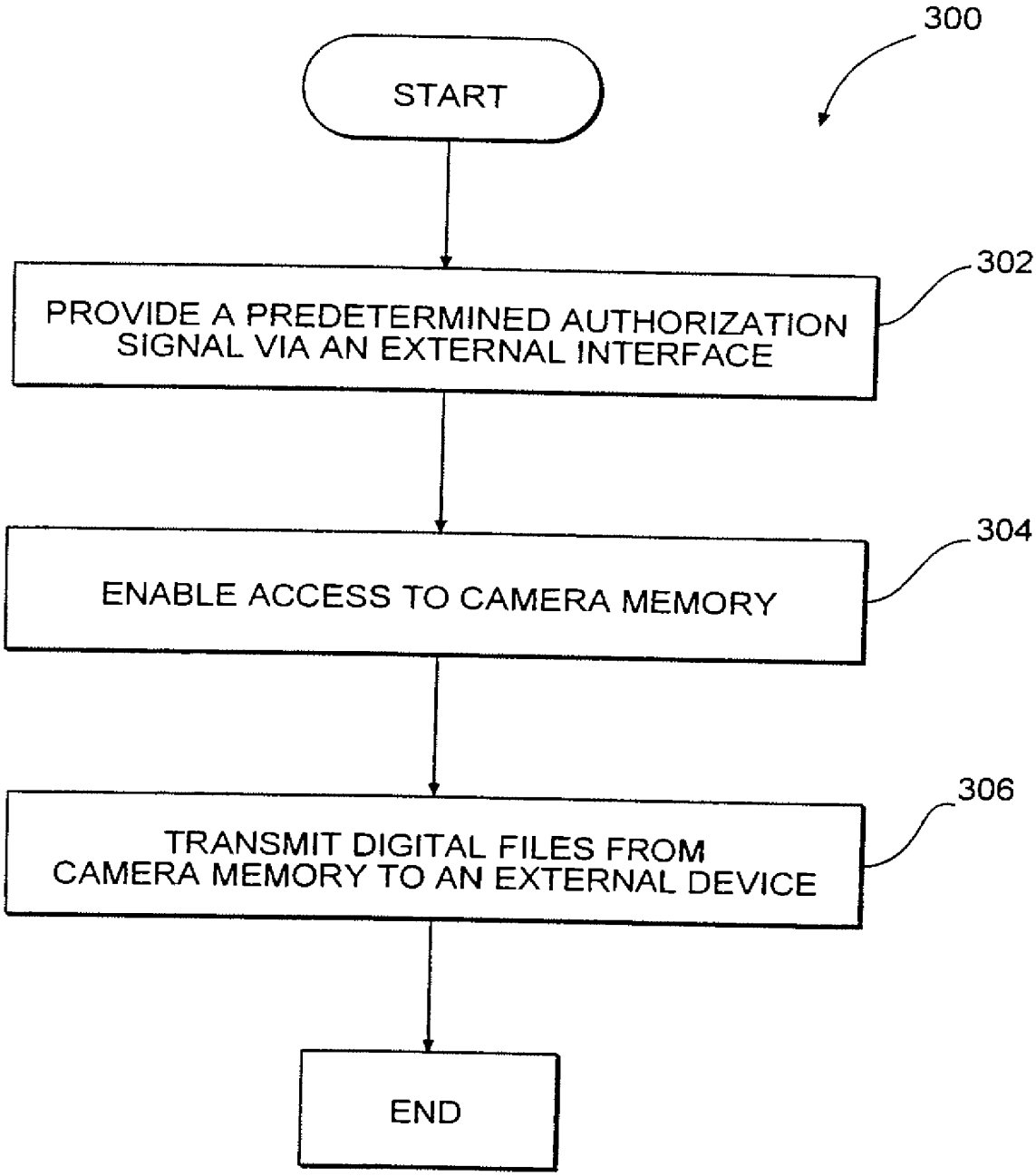

300
START
PROVIDE A PREDETERMINED AUTHORIZATION SIGNAL VIA AN EXTERNAL INTERFACE
302
ENABLE ACCESS TO CAMERA MEMORY
304
TRANSMIT DIGITAL FILES FROM CAMERA MEMORY TO AN EXTERNAL DEVICE
306
END

FIG. 3A

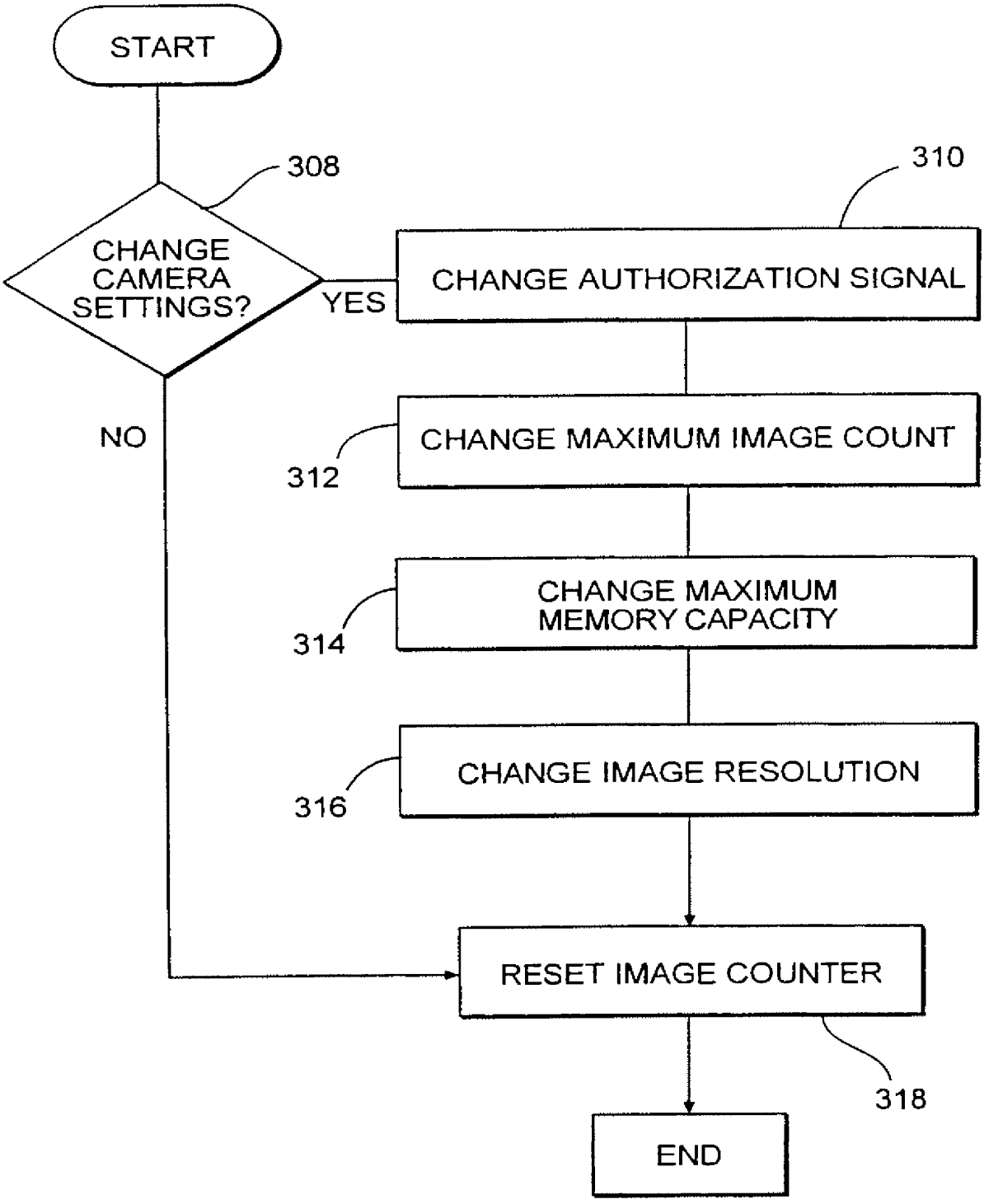

START
308
CHANGE CAMERA SETTINGS?
YES
NO
310
CHANGE AUTHORIZATION SIGNAL
312
CHANGE MAXIMUM IMAGE COUNT
314
CHANGE MAXIMUM MEMORY CAPACITY
316
CHANGE IMAGE RESOLUTION
RESET IMAGE COUNTER
318
END

FIG. 3B

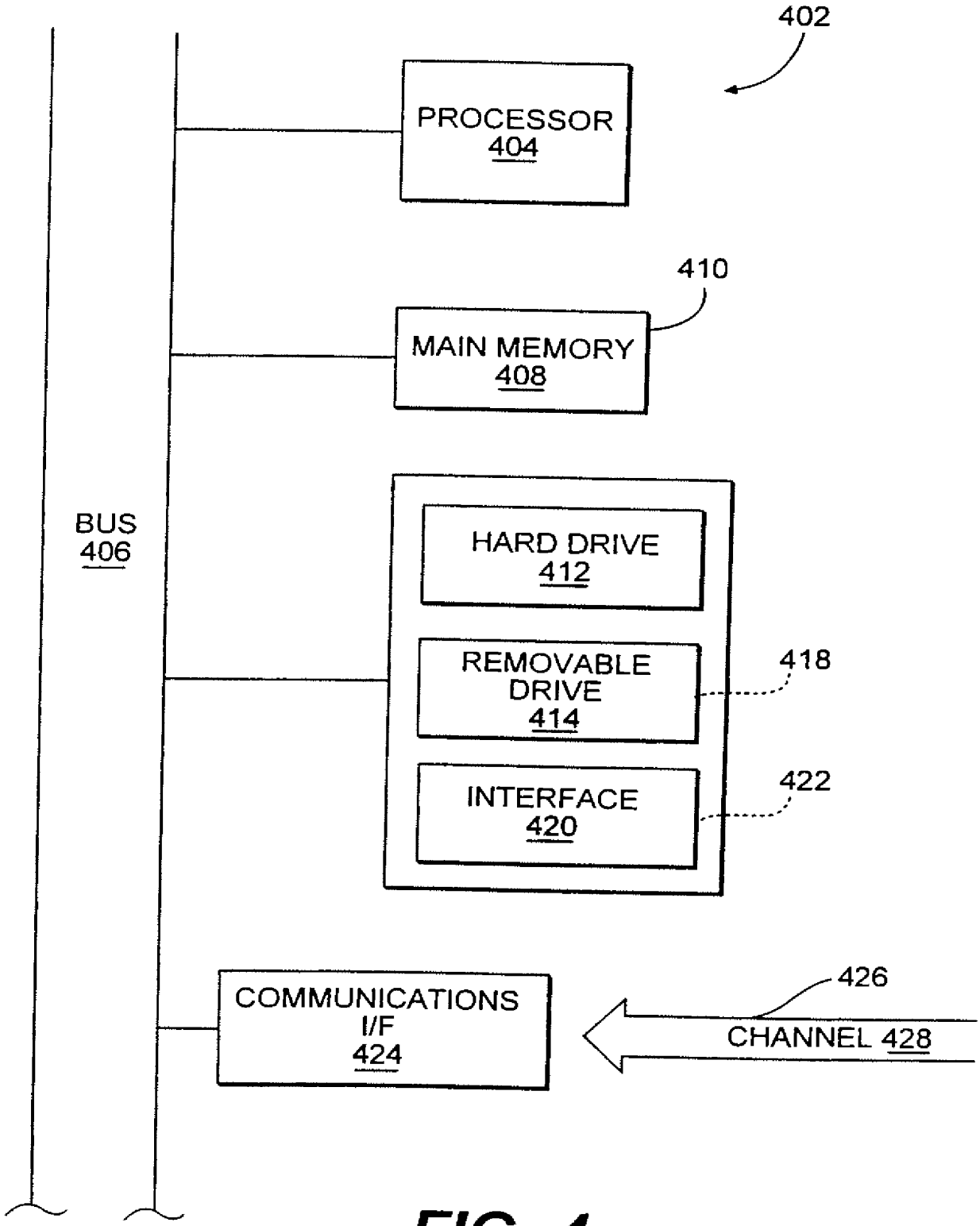

402
PROCESSOR
404
410
MAIN MEMORY
408
BUS
406
HARD DRIVE
412
REMOVABLE
DRIVE
414
418
INTERFACE
420
422
COMMUNICATIONS
I/F
424
426
CHANNEL 428

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/22353

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :
US CL :

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 348/207, 231, 232, 233; 380/200, 210, 229, 232, 243; 396/6

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
BRS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X ----- Y	US 5,898,779A (Squilla et al.) 27 April 1999 (27.04.1999), figure 2, column 4, lines 38-column 5, lines 34-40; column 6, lines 37-41; column 7, lines 21-26; figure 9, column 9, lines 22-25	1, 7-11, 16,18, 20, 24, 26, 28-34, 42, 43, 45-49, 55, 57-59, 61, 63-66, 68, 71, 72, 74, 76 --- 17, 19, 21-23, 25, 27
Y	US 5,852,467 (Ogino) 22 December 1998 (22.12.1998), figure 6, column 3, lines 54-67	13-15, 35-37, 41, 44, 52, 56, 62, 69, 73, 75
Y	US 5,699,549 (Cho) 16 December 1997 (16.12.1997), column 5, lines 45-51	12, 50, 53, 60, 67, 70

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
	02 JAN 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer WENDY GARBER Telephone No. 703-305-9048

Form PCT/ISA/210 (second sheet) (July 1998)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

REVISED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 March 2001 (01.03.2001)

PCT

(10) International Publication Number
WO 01/15440 A1

(51) International Patent Classification[7]: H04N 5/76

(21) International Application Number: PCT/US00/22353

(22) International Filing Date: 15 August 2000 (15.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/149,999 20 August 1999 (20.08.1999) US

(71) Applicant *(for all designated States except US)*: DIGITAL NOW, INC. [US/US]; Suite 140, 8401 Old Courthouse Road, Vienna, VA 22182 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: REED, William, G. [US/US]; 9804 62nd Avenue South, Seattle, WA 98118 (US).

(74) Agent: REISTER, Andrea, G.; Covington & Burling, 1201 Pennsylvania Avenue, N.W., Washington, DC 20004-2401 (US).

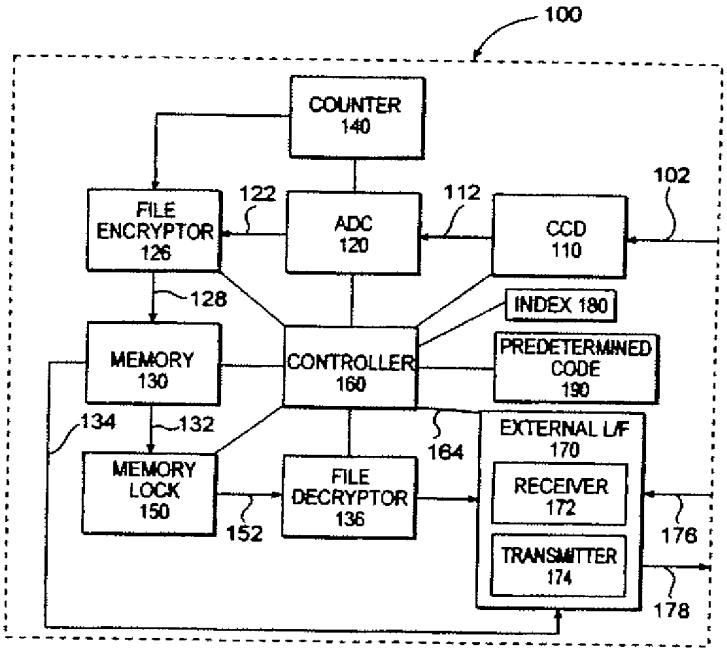
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

[Continued on next page]

(54) Title: ONE TIME USE DIGITAL CAMERA



(57) Abstract: Apparatus and method for preventing unauthorized access or erasure of digital image files stored in the memory (130) of a digital camera (100) used for taking motion still photographs, motion pictures, etc., while permitting an authorized person to access, erase and/or reset the camera (100) for further use. Access and erasure of the digital files is enabled only when a predetermined authorization signal (126), code or decryption key (136) is received via an external interface (170).

WO 01/15440 A1

(88) **Date of publication of the revised international search report:** 12 July 2001

(15) **Information about Correction:**
see PCT Gazette No. 28/2001 of 12 July 2001, Section II

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

REVISED VERSION

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/22353

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04N 5/76
US CL : 348/207, 231, 232, 233; 380, 200210, 229, 232, 243; 396/6

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 348/207, 231, 232, 233; 380/200, 210, 229, 232, 243; 396/6

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
BRS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X ----- Y	US 5,898,779A (Squilla et al.) 27 April 1999 (27.04.1999), figure 2, column 4, lines 38-column 5, lines 34-40; column 6, lines 37-41; column 7, lines 21-26; figure 9, column 9, lines 22-25	1, 7-11, 16,18, 20, 24, 26, 28-34, 42, 43, 45-49, 55, 57-59, 61, 63-66, 68, 71, 72, 74, 76 --- 17, 19, 21-23, 25, 27
Y	US 5,852,467 (Ogino) 22 December 1998 (22.12.1998), figure 6, column 3, lines 54-67	13-15, 35-37, 41, 44, 52, 56, 62, 69, 73, 75
Y	US 5,699,549 (Cho) 16 December 1997 (16.12.1997), column 5, lines 45-51	12, 50, 53, 60, 67, 70

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
	19 MAR 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer WENDY GARBER Telephone No. 703-305-9048

Form PCT/ISA/210 (second sheet) (July 1998)